SYMPA HR – 100% GDPR compliant

Fully GDPR compliant? How we do it?

With the 25 May 2018, the date on which GDPR comes into force, fast approaching, we wanted to put your mind at ease and explain in detail how your Sympa HR system is already fully compliant with the new regulations.

To summarise, the spirit of GDPR is to keep your personal data up-to-date, secure and available for those who need it. Here's how we've implemented this spirit in practice to create a fully GDPR compliant HR system.

Flexible GDPR support

We've actively developed our GDPR processes and support materials to support your compliancy as well. Helpful GDPR material is publicly available at Sympa GDPR website and in more detail for customers only at Sympa HR Support Portal.

As a company, we value privacy and security highly and subscribe to the *Privacy by Design* principles behind GDPR.

That's why we've developed Sympa HR over the years to be fully compliant with GDPR and beyond, for 2019 and into the future. Our customers therefore have little to worry about GDPR when it comes to their HR system being compliant.

Finally, it's fair to say out loud that GDPR is new to many of us. The best practice and guidance available from the authorities are constantly changing and improving. We welcome all feedback and are happy to help in any GDPR related questions in HR, so feel free to contact any of us at Sympa! We look forward to hearing from you.

Technical specifications, Sympa HR & GDPR Compliancy

To ensure we are on the same page about GDPR and our common GDPR compliancy, we have prepared a technical specification sheet for you. Please study the pdf document, downloadable below, and let us know if you have any questions.

Enjoy the technical details!

Keijo Karjalainen
CEO & Founder
+358 40 521 8517
keijo.karjalainen@sympa.com

SYMPA HR – 100% GDPR compliant

How do we do it?

SYMPA HR: THE COMPREHENSIVE HR SYSTEM
Technopolis Helsinki-Vantaa · Teknobulevardi 3–5, 01530 Vantaa, Finland
+358 290 001 200 · sympa.com · Domicile: Lahti, Finland · Business ID: FI19385975

v. 2018-01

Sympa HR & GDPR Roles

Data Controller

You, as a Sympa Customer, are a data controller. The data controller makes all the decisions about the content, processes and access to data.

Data Processor

Sympa, as a service provider, is a data processor. We process our customers' data only for the purpose of providing the Sympa HR Service. Sympa is responsible to you and also directly to the authorities.

Data Subject

Your employees are data subjects. Typically, these also include freelancers, job applicants, subcontractors, former employees and anyone else, whose data is stored and processed in Sympa HR.

Data Protection Officer (DPO)

Organizations that engage in large scale data processing are required to have a data protection officer.

Sympa HR supports Data Subjects rights

Privacy by Design

Data privacy and security are the foundation of the Sympa HR service. Our business is processing HR data. We have recognised privacy as a vital necessity for serving our clients.

Privacy is paramount in all our operations including service development, hosting, support services, implementations and also in sales and marketing. Privacy is similarly a priority in current operations and in development projects. We have built and certified our ISMS (Information Security Management System) to ISO27001 standards to demonstrate our compliance and continuous development. Our ISMS and certification covers all our operations and locations.

We continuously evaluate and develop our technical and organisational protection methods as well as risk evaluation processes for better data protection and data privacy. Privacy of your data is our key priority.

Right to be informed

All individuals have the right to be informed about when their personal data is being stored and what data is stored.

Sympa HR:

- Provides legible, easy-to-understand GDPR-proofed templates to use as data privacy documents
- An up-to-date Service Description with details about data use is always available
- In the event that any changes in the service take place that might affect your GDPR compliance, we will let you know

Right to access & Right to rectification

Individuals have the right to access their own data and right to have any incorrect data rectified.

Sympa HR:

- We are a full self-service solution. As the Data Controller, you as our customer can easily choose to make all personal data available for individuals in either read only or read&write mode.
- Our customers can also manage the rights, and only the appropriate people will have the right to see the any given piece of information
- Any access to a user's own personal data is customised according to our customers' processes
- Self-service applies also for IT integrations: you can manage which data is integrated to and from Sympa HR when integrated with other IT systems
- Sympa HR tools support right to access even in cases where an individual is not able to access Sympa HR directly. User experience upgrades are released to production before May 2018.

Right to erasure ('right to be forgotten')

Individuals have the right to have their data erased when processing is no longer necessary.

Sympa HR:

- Removing unnecessary data is a standard feature in Sympa HR and can also be automated when it supports your processes. Upgraded automation tools are released to production before May 2018.
- Data removals can also be done in several stages. Some data must be stored for longer period of time than other data (for example employment agreements vs. competencies, one-to-one discussions).
- Sympa HR data removal is always secure and disaster recovery systems support GDPR requirements.

Right to data portability

Individuals have the right to have their data provided to them in an easily readable format and also have the right to transmit that data to another controller.

Sympa HR:

- All data that is stored can be exported via the Sympa HR user interface or API.
- Sympa HR supports fast and easy way to comply with the data portability requirement (released to production before May 2018).

Breach notification

Data breaches must be reported to the authorities within 72 hours.

Sympa HR:

- Sympa HR is being monitored and protected 24/7 by separate team of security experts.
- In the unlikely event of breach, we will immediately notify you and provide our customers with instructions on how to notify authorities and data subjects

Sympa HR Meets technical and organisational GDPR requirements

Sympa HR provides secure data – at rest and in motion.

Sympa's ISMS is built to protect your data. Advanced ISMS and 3rd party information security audits and certifications are the key methods of the protection. In addition, we have identified following technical security features and operating models as key tools in information security and GDPR compliance.

Risk assessments and risk management

Risk-aware thinking is a fundamental part of Sympa's quality management (ISO9001 certified) and information security management (ISO27001 certified) systems. Risk assessment processes include identifying likelihoods, impacts and mitigation and also possibilities related to identified risks. Protection of Customers' data has been identified as the most critical asset of Sympa. Risk assessment and management processes are audited annually by a third party.

Encryption

All the data *stored in* and *transferred to/from* Sympa HR is encrypted with strong encryption algorithms, at rest and in motion.

User management, permissions and authentication

Sympa HR is an HR system where all employees are users by default. Naturally, in some cases, access to the system is limited by the user organisation. Sympa HR is the master system for HR data and typically this data is used by the client in connected IT systems and user management.

Users' access to data can be limited in the system on need-to-know basis to only include limited persons and limited data set. Typically, most of the data is accessed based on organisation hierarchy, but Sympa HR also supports tailored access rights for example for IT users.

Sympa recommends using Single Sign-On (SSO) login and authentication for best user experience and maximum security. SSO login can be used together with multifactor authentication. Sympa HR supports username+password login with password complexity requirements, where SSO is not available.

Logging

Logins and logouts, including failed login attempts are logged in detail. On data level, all data approvals are logged and Sympa HR supports storing historical and future data. All changes to data can be logged including details about who changed what and when. Sympa HR system maintenance team has access to more detailed user action logs and events, in case such data is needed.

Maintenance operations and events in hosting environment are logged and logs are protected from tampering.

Backups and disaster recovery

Sympa HR is designed and built as high availability (HA) service where all components are redundant.

Backups from the Customer data is taken daily (changes) with real-time transaction logging. Full backup is taken once per week. RPO (recovery point objective) for disaster recovery is one day. When data loss is caused by human or software error, RPO is 2 minutes.

RTO (recovery time objective) varies based on different disaster levels and is based on risk evaluation process. Loss of primary and redundant hardware has RTO of 60 minutes. RTO for full data centre loss is 7 days.

Service provider's access to data

Limited team members in Sympa HR service delivery, maintenance, security and service teams has access to data stored in Sympa HR service. Access is based on personal credentials and user actions can be tracked on detailed level if needed. Segregation of duties is implemented based on personal job descriptions. Separate security clearance takes place prior to nomination to most critical roles. The access rights are reviewed or removed regularly and when a person's job or responsibilities change or they leave the company.

Removing data

Personal data can be removed from the system by the Customer. Removed data will stay on disaster recovery systems for a while and will be removed automatically according to backup rotation cycles. Data removals are secure and no data can be restored after it has been removed from backups.

By request and at the end of customer relationship all data is securely removed from Sympa HR system and databases including backup systems. Full data removal is coordinated with the Customer in such way, that all data can be returned to Customer or transferred to another system prior to erasure.

Hosting and data locations

Our EU customers' data is stored fully within EU datacentres. The primary hosting environment is located in London, UK. Some parts of the service, including offsite backups, disaster recovery, integrations, and features such as binary storages, are delivered from secondary datacentres in the EU. Currently these locations include Germany, Ireland and the Netherlands. We are committed to keep your data within the EU's borders even after Brexit.

24/7 security services are delivered via the follow-the-sun model. This enables us to have best security experts working full time with full service availability and security topics. Teams are stationed across the world and come on-shift consecutively ensuring that responses to security incidents and threats come within seconds instead of hours. During the hours of darkness in Europe, security services and service monitoring is delivered from US under US-EU Privacy Shield agreement.

Hosting providers at the moment include Rackspace (main provider), Microsoft (Azure infrastructure) and Amazon (disaster recovery and optional integration technologies).

Sympa HR support services are delivered from Sympa's EU/EEA locations.

Integrations

Data is always transferred using secure SFTP or HTTPS protocols. Integrations can be customised to include only the necessary information. If another system (for example, your payroll system) that integrates into Sympa HR

only requires an individual's mailing address and not their social security number or any other data, Sympa HR can be customised to share only the address.

Record keeping

As the Data Controller, you will decide beforehand who has access to what information within Sympa HR. By customising user rights (per job role, for example) you can ensure that only the relevant people have access to sensitive data.

As the Data Processor, Sympa maintains a record of all categories of processing activities.

Data minimisation

Data minimisation is very much in keeping with the spirit of GDPR. Sympa HR makes it easy to customise data fields, delete (or correct) unnecessary data and keep your database lean.

We will continue to make usability improvements to the system in order to help you remain compliant, but with less effort.

Data pseudonymisation and anonymization

Sympa HR service monitoring, development and maintenance requires following user actions, system usability and HR processes. Pseudonymisation and anonymization both play an important role is Sympa HR Service delivery. Pseudonymisation and anonymization enable us to deliver the best possible HR system without using your HR data or any personally identifiable information (PII).

Data Breaches

Sympa HR's security and customer data is monitored and protected 24/7. Sympa has a clearly-defined protocol for identifying, mitigating and informing customers about any possible data breaches.

Processing of Personal Data

Sympa as the Data Processor offers and maintains an electronic HR system for the Customer (Data Controller), enabling the Customer to manage personal data including employment, salary, competencies and other personal data for employees, former employees, job applicants, freelancers, subcontractors and such interest groups at Customer's choice.

Customer collects, records, analyses and otherwise uses information stored in the HR system for its own account. Sympa does not take part in these activities except by providing a tool that enables the Customer to perform these measures and when specifically asked so by the Customer.

Sympa reviews the information stored on the HR system only to the extent necessary to maintain the system for the Customer (including, for example, correcting errors in the system and handling other technical problems in the system). Sympa does not look at the data stored in the HR system more than is necessary to maintain the HR system and related services.

Categories of processing activities are dependent on Customer's configuration. Categories include gathering data from end users and via APIs, storing data in the service and backup systems, distributing data to end users (reporting) and via APIs, organising and changing data according to Customer's instructions.

Other GDPR actions by Sympa

Sympa follows a process of continuous development.

Education and training

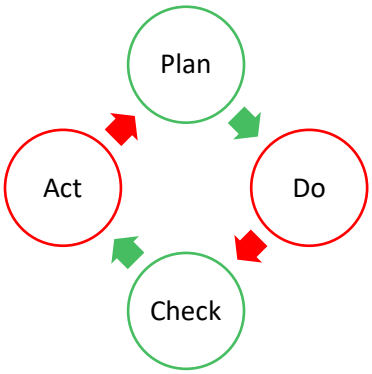
All Sympa employees are trained in GDPR so your contact person will be happy to help. You can also try our Support Service, which available by phone, emails and via the Support Portal, which has up-to-date materials available 24/7.

Updated agreements

GDPR requirements are covered in Sympa HR agreements by default, however small updates may be necessary. We will contact you regarding any updated agreement.

Information security management

The Sympa information security organization is led by Sympa's information security manager and DPO Tommi Surakka. Our security organisation takes care of Sympa's information security management system (ISMS) including continuous development, risk assessments, information security audits, training and 24/7 monitoring and incident management. Sympa's most critical asset is its customers' data and we are fully aware of that fact.



An overview of security organization and security groups is outlined below. (ISMS controls A6)

Continuous development in P-D-C-A cycles has been the key driver for Sympa HR information security management. Sympa was first granted ISO27001 certification for excellence in information security in 2014 and Sympa has been continually certified since then. The certificate was conferred by Bureau Veritas. Certification covers all operations and locations. The certificate and statement of applicability are available on request.

Sympa HR information security roles and teams in light red boxes. **Information security audits** in light green boxes.

Information Security Manager
- Responsible for Sympa's ISMS

Data Protection Officer
- Monitoring data protection and privacy

Information Security Management Group
- Continuous ISMS development
- Change management
- Regular meetings
- Incident management

Technical Information Security Group
- Technical information security
- Technical security architechture
- Technical security reviews
- Information security code reviews

24/7 Information Security Team
- Monitoring information security and protecting data 24/7
- Rapid response to threats 24/7
- Availability monitoring and repairs 24/7
- Vulnerability scanning
- Security patches,platform and infrastructure management

System Operators
- Proactive security and availability management
- Release management
- Technical information security planning and management in production environment

Internal ISMS audits
- Annual detailed information security audits
- Follow multi-year plan for continuous development
- Audit duration 5–10 days per year

External information security audits
- ISMS is audited against ISO27001 and ISO9001 standards
- Certification since 2014
- Audit duration 3–7 days per year

Technical information security audits
- 3rd party audits for technical information security
- Audits are performed before any major change in Sympa HR Service
- Audits are performed minimum once per year
- Audit duration 5+ days per year

Information security controls

Sympa's ISMS covers all operations and locations. Sympa's Information Security Policy (ISMS controls A5.1) is reviewed regularly and is available for review on request. An overview of Sympa's Information Security Management System and the most relevant controls is provided below. A more extensive list of controls is available on request (statement of applicability). Controls have been chosen to meet ISO27001 standards.

Human Resources (ISMS controls A7)

Prior to employment all employees go through interview and screening processes. Depending on the role, and when roles are changed, more detailed screening process may take place. Police security clearances are performed where applicable. All employees sign a non-disclosure agreement before joining Sympa.

During employment security and privacy awareness is supported by our training programs. At the end of employment Sympa's exit process includes access terminations, asset management, change management and interviews to support continuous development.

Asset management (ISMS controls A8)

Asset management includes processes and tools for asset inventory, ownership, data classification as well as guidelines and policies for acceptable use, physical media handling and disposals. The nature of our work means that travelling and working from remote locations is common practice. Our asset protection is based primarily on encryption and protection methods that are location-independent.

Access control (ISMS controls A9)

Sympa's user management and access rights rely on up-to-date HR and subcontractor data managed with Sympa HR. All access and user management processes include named responsibilities and regular reviews. Access to most critical systems is very limited, on a need-to-know basis and protected accordingly, taking into account best practices in multi-factor authentication, restrictions and logging.

Cryptography (ISMS controls A10)

Cryptography is recognized as one of the most important protection methods in technical information security. All critical data is always encrypted in motion and at rest. Special attention is paid to transactions and communication with Sympa HR client organisations and unsecure tools, such as email, are deprecated.

Physical security (ISMS controls A11)

Sympa HR service and critical data is stored in the most secure physical environments. To offer the best possible physical security Sympa has chosen the best hosting providers available. Current hosting environment certifications include ISO27001, PCI-DSS and SSAE16 Type II SOC1, SOC2, SOC3. Access is restricted by biometric authentication, keycards, and 24x7x365 surveillance. Hosting locations are staffed with 24/7 onsite security teams.

Operations security (ISMS controls A12)

Operational safety is based on documented procedures, responsibilities and change and capacity management. Development, testing and production environments are isolated and customers' data is not used in development or testing environments.

Operational environments are protected against malware, information is backed up, operational events are logged and logs are protected against tampering. Installation of software on operational environments are limited and controlled accordingly.

Sympa's operations and information systems are audited regularly. Vulnerabilities are managed and audited in relation to change management and at least annually to ensure protection against advanced and evolved vulnerability exploits.

Communications security (ISMS controls A13)

All confidential electronic information transfers are encrypted with strong encryption when not transferred within high security isolated networks. All confidential transfers in public internet are encrypted. Networks are always isolated where feasible. Human communications are protected with confidentiality and non-disclosure agreements.

Development & Maintenance (ISMS controls A14)

Development and maintenance processes are monitored carefully by security team. Product architecture, design and development efforts are evaluated by separate technical security team. All changes in software are always reviewed before approval to releases. All changes in software, including third party component changes are logged and can be tracked in detail. Quality assurance / testing processes also include security testing and vulnerability scanning and management.

Supplier relations (ISMS controls A15)

Sympa takes full responsibility for its suppliers and subcontractors. Risks related to supplier relations are mitigated with security policies, security practices and guides, supplier agreements including confidentiality and non-disclosure statements. Residual risks are mitigated with information security insurances.

Incident management (ISMS controls A16)

Information security incidents, improvements, opportunities and feedback are booked and handled according to documented practices. Processes vary by criticality where critical events are handled immediately and low priority events are handled in regular information security group meetings. All persons related to service delivery are aware of incident management practises.

Business continuity (ISMS controls A17)

Sympa's business continuity is focussed on Sympa HR information security and service continuity. Identifying continuity risks and opportunities form the most critical part of Sympa's ISMS. Continuity is ensured with careful planning, reviews and regular third-party audits.

Sympa HR service continuity planning is based on high-availability design and fully redundant infrastructure.

Compliance (ISMS controls A18)

Compliance with applicable laws, regulations, authorities' guides and contractual requirements. Special attention is paid on intellectual property rights and regulations related to handling personally identifiable information (PII).

Compliance in information security is reviewed regularly by independent third party.

SUMMARY

GDPR cooperation – Processor responsibilities that we guarantee for our customers as our role of Data Processor

- Sympa, as the Processor, will immediately inform the controller in the unlikely event that we believe that the controller's instructions conflict with the requirements of the GDPR or other EU or Member State laws
- Sympa, as the Processor, must and has implemented measures to assist the controller in complying with the rights of data subjects
- Sympa, as the Processor, must and will assist the controller in obtaining approval from DPAs where required
- Sympa, as the Processor, must and will return or destroy the personal data at the end of the relationship in cooperation with the controller
- Sympa, as the Processor, must and will provide the controller with all information necessary to demonstrate compliance with the GDPR
- Sympa, as the Processor, must will notify the controller of any data breach without undue delay
- Data subjects can bring claims directly against processors (Sympa)

Sympa HR is 100% GDPR-compliant now and into the future.

We will develop our product as GDPR – or any other EU's regulation – progresses. As our customer, you can be sure that you always have a secure, safe and security compliant solution, where your employee data is kept up-to-date and safe.

Examples of our ongoing efforts to ensure future GDPR compliance:

- On-going reviews of security measures
- Ensuring redundancy and back-ups
- Performing regular security tests

GDPR requires you to have up-to-date HR data available to those who need it, when they need it. - How cool is that?.

CONTACT

If you have questions, or interesting information, don't hesitate – get in touch!

We'd love to think we could know it all, but we're smart enough to know we can't so we're always happy to learn.

Henrikki Kainulainen
Customer Success Director
+358 50 537 4727
henrikki.kainulainen@sympa.com

Tommi Surakka
Data Protection Officer (DPO)
+358 50 430 8360
tommi.surakka@sympa.com

Mikko Kojo
Product Director
+358 50 371 7975
mikko.kojo@sympa.com

Keijo Karjalainen
CEO & Founder
+358 40 521 8517
keijo.karjalainen@sympa.com